PENDING CLAIMS

1. (Previously Amended) A method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device, and said method comprising:

partitioning at least a portion of said storage device to form a security partition having at least one authority record and at least one data set associated with said authority record; and

limiting access to the security partition of said storage device by said operating system of said computer system.

2. (Original) The method of Claim 1, wherein said computer system includes a networked computer system.

3. (Original) The method of Claim 1, wherein at least a portion of said storage device firmware comprises writeable firmware.

4. (Original) The method of Claim 1, wherein at least a portion of said storage device firmware comprises non-writeable firmware.

5. (Original) The method of Claim 1, further comprising transporting data to said storage device only in connection with execution of said firmware of said storage device.

6. (Original) The method of Claim 1, wherein said storage device is configured in accordance with a protocol selected from the group consisting of ATA protocol and SCSI protocol.

7. (Original) The method of Claim 1, wherein said partitioning steps occurs on a low-level formatting portion of said storage

device.

8. (Original) The method of Claim 1, further comprising adding data to said storage device in an orientation selected for promoting identification of remaining data storage space on said storage device.

9. (Original) The method of Claim 1, further comprising said security partition having a master authority record.

10. (Original) The method of Claim 9, further comprising said master authority record governing all said authority records in said storage device.

11. (Original) The method of Claim 1, further comprising translating information from a master authority record included in said storage device to a group authority in said operating system.

12. (Original) The method of Claim 1, further comprising writing said security partition using a security partition open call.

13. (Original) The method of Claim 12, further comprising closing said security partition after a predetermined time interval.

14. (Original) The method of Claim 1, further comprising reading said security partition using a security partition open call.

15. (Original) The method of Claim 14, further comprising closing said security partition after a predetermined time interval.

16. (Original) The method of Claim 1, wherein said authority record includes a public-private key pair for authenticating data

originating from said security partition.

17. (Original) The method of Claim 16, wherein said authority record includes a second public-private key pair for ensuring data can only be sent to said security partition and no other location for storing said data.

18. (Original) The method of Claim 1, further comprising storing a symmetric key on said storage device.

19. (Original) The method of Claim 1, further comprising using a private key for decoding a passcode transmitted to said authority record of said storage device.

20. (Original) The method of Claim 1, further comprising encrypting at least a portion of said data in said security partition.

21. (Original) The method of Claim 1, further comprising encrypting data on said storage device so that only an external agent can decrypt said encrypted data.

22. (Original) The method of Claim 1, further comprising providing no method for decrypting data stored on said storage device with information available on said storage device.

23. (Original) The method of Claim 1, further comprising hiding at least one field of said authority record.

24. (Original) The method of Claim 1, further comprising storing a hash of code in a passcode field of said authority record.

25. (Original) The method of Claim 1, further comprising securing

a symmetric key by encrypting said symmetric key with a public key of said authority record, and hiding a private key in said authority record, thereby permitting only said hidden private key to decode said symmetric key.

26. (Original) The method of Claim 1, further comprising storing at least one public key in said storage device.

27. (Original) The method of Claim 1, further comprising storing at least one private key in said storage device.

28. (Original) The method of Claim 1, further comprising declaring at least a portion of data in said security partition to be write-once.

29. (Original) The method of Claim 1, further comprising permitting only a predetermined user to access a master authority record of said security partition.

30. (Original) The method of Claim 1, wherein said authority record includes at least one nonce.

31. (Original) The method of Claim 30, further comprising encrypting said nonce with a public key.

32. (Original) The method of Claim 1, wherein said authority record includes at least one time value associated with processing of a portion of data stored on said storage device.

33. (Original) The method of Claim 32, wherein said time value is selected from the group consisting of a start time and an end time.

34. (Original) The method of Claim 1, further comprising storing call authentication data on said storage device.

35. (Original) A system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device, said system for promoting security comprising:

a security partition formed in said storage device having at least one authority record and at least one data set associated with said authority record;

wherein access to said partition in said storage device by said operating system of said computer system is limited.

36. (Original) The system of Claim 35, wherein said computer system includes a networked computer system.

37. (Original) The system of Claim 35, wherein at least a portion of said storage device firmware comprises writeable firmware.

38. (Original) The system of Claim 35, wherein at least a portion of said storage device firmware comprises non-writeable firmware.

39. (Original) The system of Claim 35, wherein said storage device is configured in accordance with a protocol selected from the group consisting of ATA protocol and SCSI protocol.

40. (Original) The system of Claim 35, wherein said security partition is formed on a low-level formatting portion of said storage device.

41. (Original) The system of Claim 35, further comprising said security partition having a master authority record.

42. (Original) The system of Claim 41, further comprising said master authority record being in operative association with a group authority in said operating system.

43. (Original) The system of Claim 35, wherein said authority record includes a public-private key pair for ensuring data can only be sent to said security partition.

44. (Original) The system of Claim 43, wherein said authority record includes a second public-private key pair for ensuring data can only be sent to said security partition and no other location for storing said data.

45. (Original) The system of Claim 35, further comprising a symmetric key stored on said storage device.

46. (Original) The system of Claim 35, further comprising encrypted data stored on said storage device.

47. (Original) The system of Claim 35, further comprising at least one hidden field in said authority record.

48. (Original) The system of Claim 35, further comprising said authority record having a passcode field.

49. (Original) The system of Claim 35, further comprising a hidden key stored in said storage device.

50. (Original) The system of Claim 35, further comprising at least one public key stored in said storage device.

51. (Original) The system of Claim 35, further comprising at

least one private key stored in said storage device.

52. (Original) The system of Claim 35, wherein said authority record includes at least one nonce.

53. (Original) The system of Claim 35, wherein said authority record includes at least one time value associated with processing of a portion of data stored on said storage device.

54. (Original) The system of Claim 53, wherein said time value is selected from the group consisting of a start time and an end time.

55. (Original) The system of Claim 35, further comprising call authentication data stored on said storage device.

56. (Original) A computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device, said medium comprising:

instructions for partitioning at least a portion of said storage device to form a security partition having at least one authority record and at least one data set associated with said authority record;

instruction for limiting access to at least a portion of said storage device by said operating system of said computer system.

57. (Original) The medium of Claim 56, wherein said computer system includes a networked computer system.

58. (Original) The medium of Claim 56, wherein at least a portion of said storage device firmware comprises writeable firmware.

59. (Original) The medium of Claim 56, wherein at least a portion of said storage device firmware comprises non-writeable firmware.

60. (Original) The medium of Claim 56, further comprising instructions for transporting data to said storage device only in connection with execution of said firmware of said storage device.

61. (Original) The medium of Claim 56, wherein said storage device is configured in accordance with a protocol selected from the group consisting of ATA protocol and SCSI protocol.

62. (Original) The medium of Claim 56, wherein said instruction for partitioning include instruction for partitioning in a low-level formatting portion of said storage device.

63. (Original) The medium of Claim 56, further comprising instructions for adding data to said storage device in an orientation selected for promoting identification of remaining data storage space on said storage device.

64. (Original) The medium of Claim 56, further comprising said security partition having a master authority record.

65. (Original) The medium of Claim 64, further comprising said master authority record including instructions for governing all said authority records in said storage device.

66. (Original) The medium of Claim 56, further comprising instructions for translating information from a master authority

record included in said storage device to a group authority in said operating system.

67. (Original) The medium of Claim 56, further comprising instructions for writing said security partition using a security partition open call.

68. (Original) The medium of Claim 67, further comprising instructions for closing said security partition after a predetermined time interval.

69. (Original) The medium of Claim 56, further comprising instructions for reading said security partition using a security partition open call.

70. (Original) The medium of Claim 69, further comprising instructions for closing said security partition after a predetermined time interval.

71. (Original) The medium of Claim 56, wherein said authority record includes a public-private key pair for authenticating data originating from said security partition.

72. (Original) The medium of Claim 71, wherein said authority record includes a second public-private key pair for ensuring data can only be sent to said security partition and no other location for storing said data.

73. (Original) The medium of Claim 56, further comprising instructions for storing a symmetric key on said storage device.

74. (Original) The medium of Claim 56, further comprising instructions for using a private key for decoding a passcode

transmitted to said authority record of said storage device.

75. (Original) The medium of Claim 56, further comprising instructions for encrypting at least a portion of said data in said security partition.

76. (Original) The medium of Claim 56, further comprising instructions for encrypting data on said storage device so that only an external agent can decrypt said encrypted data.

77. (Original) The medium of Claim 56, further comprising instructions for hiding at least one field of said authority record.

78. (Original) The medium of Claim 56, further comprising instructions for storing a hash of code in a passcode field of said authority record.

79. (Original) The medium of Claim 56, further comprising instructions for securing a symmetric key by encrypting said symmetric key with a public key of said authority record, and instructions for hiding a private key in said authority record, thereby permitting only said hidden private key to decode said symmetric key.

80. (Original) The medium of Claim 56, further comprising instructions for storing at least one public key in said storage device.

81. (Original) The medium of Claim 56, further comprising instructions for storing at least one private key in said storage device.

82. (Original) The medium of Claim 56, further comprising instructions for declaring at least a portion of data in said security partition to be write-once.

83. (Original) The medium of Claim 56, further comprising instructions for permitting only a predetermined user to access a master authority record of said security partition.

84. (Original) The medium of Claim 56, wherein said authority record includes at least one nonce.

85. (Original) The medium of Claim 84, further comprising instructions for encrypting said nonce with a public key.

86. (Original) The medium of Claim 56, wherein said authority record includes at least one time value associated with processing of a portion of data stored on said storage device.

87. (Original) The medium of Claim 86, wherein said time value is selected from the group consisting of a start time and an end time.

88. (Original) The medium of Claim 56, further comprising of instructions for storing call authentication data on said storage device.

89. (Previously Amended) A system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device, said system for promoting security comprising:

means for partitioning at least a portion of said

storage device to form a security partition having at least one authority record and at least one data set associated with said authority record; and

means for limiting access to the security partition of said storage device by said operating system of said computer system.

90. (Original) The system of Claim 89, wherein said computer system includes a networked computer system.

91. (Original) The system of Claim 89, wherein at least a portion of said storage device firmware comprises writeable firmware.

92. (Original) The system of Claim 89, wherein at least a portion of said storage device firmware comprises non-writeable firmware.

93. (Original) The system of Claim 89, further comprising means for transporting data to said storage device only in connection with execution of said firmware of said storage device.

94. (Original) The system of Claim 89, wherein said storage device is configured in accordance with protocol selected from the group consisting of ATA protocol and SCSI protocol.

95. (Original) The system of Claim 89, wherein said means for partitioning partitions a low-level formatting portion of said storage device.

96. (Original) The system of Claim 89, further comprising means for adding data to said storage device in an orientation selected for promoting identification of remaining data storage space on said storage device.

97. (Original) The system of Claim 89, further comprising said security partition having a master authority record.

98. (Original) The system of Claim 97, further comprising means for said master authority record to govern all said authority records in said storage device.

99. (Original) The system of Claim 89, further comprising means for translating information from a master authority record included in said storage device to a group authority in said operating system.

100. (Original) The system of Claim 89, further comprising means for writing said security partition using a security partition open call.

101. (Original) The system of Claim 100, further comprising means for closing said security partition after a predetermined time interval.

102. (Original) The system of Claim 89, further comprising means for reading said security partition using a security partition open call.

103. (Original) The system of Claim 102, further comprising means for closing said security partition after a predetermined time interval.

104. (Original) The system of Claim 89, wherein said authority record includes a public-private key pair for authenticating data originating from said security partition.

105. (Original) The system of Claim 104, wherein said authority record includes a second public-private key pair for ensuring data can only be sent to said security partition and no other location for storing said data.

106. (Original) The system of Claim 89, further comprising means for storing a symmetric key on said storage device.

107. (Original) The system of Claim 89, further comprising means for using a private key for decoding a passcode transmitted to said authority record of said storage device.

108. (Original) The system of Claim 89, further comprising means for encrypting at least a portion of said data in said security partition.

109. (Original) The system of Claim 89, further comprising means for encrypting data on said storage device to that only an external agent can decrypt said encrypted data.

110. (Original) The system of Claim 89, further comprising means for providing no system for decrypting data stored on said storage device with information available on said storage device.

111. (Original) The system of Claim 89, further comprising means for hiding at least one field of said authority record.

112. (Original) The system of Claim 89, further comprising means for storing a hash of code in a passcode field of said authority record.

113. (Original) The system of Claim 89, further comprising means for securing a symmetric key by encrypting said symmetric

key with a public key of said authority record, and means for hiding a private key in said authority record, thereby permitting only said hidden private key to decode said symmetric key.

114. (Original) The system of Claim 89, further comprising means for storing at least one public key in said storage device.

115. (Original) The system of Claim 89, further comprising means for storing at least one private key in said storage device.

116. (Original) The system of Claim 89, further comprising means for declaring at least a portion of data in said security partition to be write-once.

117. (Original) The system of Claim 89, further comprising means for permitting only a predetermined user to access a master authority record of said security partition.

118. (Original) The system of Claim 89, wherein said authority record includes at least one nonce.

119. (Original) The system of Claim 118, further comprising means for encrypting said nonce with a public key.

120. (Original) The system of Claim 89, wherein said authority record includes at least one time value associated with processing of a portion of data stored on said storage device.

121. (Original) The system of Claim 120, wherein said time value is selected from the group consisting of a start time and an end time.

122. (Original) The system of Claim 89, further comprising means for storing call authentication data on said storage device.

123. (Previously Added) A storage device for promoting security in a computer system, the storage device comprising:

a storage medium for storing data;

firmware for reading data from and writing data to the storage medium; and

a partition defined on the storage medium for dividing the storage medium into a data partition and a secure data partition, the secure data partition for storing secure data and one or more authority records;

wherein only the firmware is permitted to access the secure data and the one or more authority records.

124. (Newly Added) The storage device of claim 123 wherein the one or more authority records includes one master authority record.

125. (Previously Added) The storage device of claim 123 wherein the storage device is in communication with a computer system having an operating system.

126. (Previously Added) The storage device of claim 125, wherein secure data stored in the secure data partition is invisible to the operating system.

127. (Previously Added) The storage device of claim 123, wherein the one or more authority records define access permissions relating to the secure data partition and the secure data.

128. (Previously Added) The storage device of claim 127, wherein the secure data partition contains a master authority record, wherein the one or more authority records can be created and deleted as required by a user having access permissions according to the master authority record.

137~~128~~. (Currently Amended) The storage device of claim 123, wherein the secure data is accessed by the firmware using a security partition open call internal to the storage device and hidden from a user.

129. (Previously Added) The storage device of claim 123 wherein each of the one or more authority records contains one public-private key pair for authenticating data that originates from the security partition.

130. (Previously Added) The storage device of claim 123, wherein the storage device further comprises:

cryptographic operations embedded in the firmware of the storage device.

131. (Currently Amended) The storage device of claim 130, wherein cryptographic code is authenticated with a root assurance in the firmware ~~of the~~ of the device, wherein the firmware is non-writable.

132. (Previously Added) A method for promoting security in a computer system having an operating system in operative connection with a storage device, wherein said storage device includes a processor and firmware for processing data stored on the storage device, the method comprising:

partitioning a storage medium of the storage device into a data partition and a secure data partition,

the data partition being accessible to a user and the secure data partition being invisible to the user, the secure data partition for storing secure data and one or more authority records; and

restricting access to the secure data partition such that only the firmware may access the secure data and the one or more authority records.

133. (Previously Added) The method of claim 132, further comprising:

prohibiting access to the secure data partition by the operating system of the computer system.

134. (Previously Added) The method of claim 133, wherein a portion of the firmware is non-writable.

135. (Previously Added) The method of claim 132, further comprising:

writing data to the secure data partition by executing of a portion of the firmware of the storage device; and

associating the data with a particular record of the one or more authority records.

136. (Previously Added) The method of claim 132 wherein the secure data is encrypted and wherein cryptographic code is embedded in the firmware, the method further comprising: authenticating the cryptographic code with a root assurance in the storage device.

138. (New) The system of claim 89 wherein the means for partitioning comprises a computer readable medium containing instructions for partitioning the storage device.

139. (New) The system of claim 89 wherein the means for limiting access to the security partition comprises the processor within the storage device, the processor adapted to limit access to the security partition according to the at least one authority record.

140. (New) The system of claim 89 wherein the means for limiting access to the security partition comprises the firmware within the storage device, the firmware adapted to limit access to the security partition according to the at least one authority record.

141. (New) A storage device comprising:

a storage medium having a security partition containing one or more authority records and at least one data set associated with each of the one or more authority records; and

a mechanism within the storage device adapted to limit access to the security partition based on the one or more authority records.

142. (New) The storage device of claim 141 wherein the mechanism comprises:

a processor disposed within the storage device adapted to limit access to the security partition by an operating system of a computer system.

143. (New) The storage device of claim 141 wherein the mechanism comprises:

firmware disposed within the storage device adapted to limit access to the security partition by an operating system of a computer system.

144. (New) The storage device of claim 141 wherein the one or more authority records comprises a master authority record including instructions for governing the one or more authority records in said storage device.

145. (New) The storage device of claim 141 wherein each of the one or more authority records comprises a plurality of fields, wherein a first field of the plurality of fields contains access rights governing access to the at least one data set.